MFT 3.4.0.0 Server Installation and Upgrade Guide

MFT 3.4.0.0 Server Installation and Upgrade Guide

Publication date 2019-11-05

EquiSign
76 route de la Demi-Lune
Les Collines de l'arche
92057 Paris La Défense Cedex-France
France
www.equisign.fr

Copyright © 2019 EquiSign. All Rights Reserved.

This product, including its related documentation, is protected by copyright and may be protected by patent.

Restricted Rights. This product, including its associated documentation, is intended to be used exclusively by holders of valid EquiSign licenses for the products documented herein. No part of this document may be reproduced or transmitted, in any form or by any means, without the prior written consent of EquiSign.

Limited Liability. While the utmost precaution has been taken in the preparation of this documentation, EquiSign assumes no responsibility for errors or omissions in this documentation. Information in this document is subject to change without notice and does not represent a guarantee on the part of EquiSign. The documentation is provided "as is" without warranty of merchantability or fitness for a particular purpose. Furthermore, EquiSign does not warrant, guarantee, or make any representations regarding the use, or the results of the use, of the documentation in terms of correctness, accuracy, reliability, or otherwise.

Trademarks and Trade Name. EquiSign® is a registered trademark of EquiSign SAS in the United States and other countries. EquiSign is a trade name of EquiSign SAS in the United States and other countries.

All other brand or product names referred to in this document are registered trademarks, trademarks, service marks, or trade names of their respective owners.

Third-party Reference Documentation. The information contained in this document is not yet part of the standard EquiSign documentation set or is intended to be a reference guide for integrating EquiSign products with third-party software. As such, it is not officially supported or maintained by EquiSign and will not necessarily be updated on the same release schedule as officially supported EquiSign products and their associated documentation.

Pre-release Documentation. The information contained in this document is not yet part of the standard EquiSign documentation set or is intended to be a reference guide for integrating EquiSign products with third-party software. As such, it is not officially supported or maintained by EquiSign and will not necessarily be updated on the same release schedule as officially supported EquiSign products and their associated documentation.

Supplemental Documentation. The information contained in this document is not yet part of the standard EquiSign documentation set or is intended to be a reference guide for integrating EquiSign products with third-party software. As such, it is not officially supported or maintained by EquiSign and will not necessarily be updated on the same release schedule as officially supported EquiSign products and their associated documentation.

Developer Documentation. The information contained in this document was written for developers by developers as a reference tool. It will not necessarily be updated on the same release schedule as EquiSign products and their associated documentation.

Table of Contents

Preface iv
1. Resources iv
1.1. Contact Customer Service iv
1.2. Contact Professional Services iv
1.3. Provide Documentation Feedback iv
2. Document Conventions iv
1. Installation Architecture Overview 1
2. Install 2
2.1. Prepare for Installation 2
2.2. Run the Installer 3
2.3. Complete the Installer Screens 4
2.4. Initialize the Server Application 6
2.4.1. Enable Anti-virus Updates via Proxy 7
2.4.2. Run the Initialization Script for Multi-host and Advanced Single-host Installations 7
2.4.3. Run the Initialization Script for Simple Single-host Installations 17
2.4.4. Configure the Network File System 18
2.4.5. Start the Managed File Transfer Application 20
2.5. Installation of the service pack 21
3. Upgrade 22
3.1. EquiSign Maintenance Upgrade Policy 22
3.1.1. Overview of Files to Be Maintained 22
3.1.2. Customer Responsibilities 22
3.1.3. Security Patches 23
3.1.4. EquiSign Support for Third-party RPM Packages Included in EquiSign Installation Packages 23
3.2. Upgrade to the lastest Product Release from 3.3.6.4 release 23
3.2.1. Supported Upgrade Paths 23
3.2.2. Upgrade Server Application, Add New Components or Features, or Change System Settings 24
3.3. Upgrade to the 3.3.6.4 Product Release or Update Server Application 25
3.3.1. Supported Upgrade Paths 25
3.3.2. Upgrade Server Application, Add New Components or Features, or Change System Settings 25
3.4. Upgrade Supported Middleware, Software, Etc. 28

Preface

The following sections contain preface information:

- Section 1, “Resources”
- Section 2, “Document Conventions”

1. Resources

Please use the information provided to contact the appropriate EquiSign department or representative.

1.1. Contact Customer Service

Support Web Site, including the Support Download Site	`https://support.equisign.fr/` (Login requires a username and password)
Email	`<support@equisign.fr>`

1.2. Contact Professional Services

Email	`<support@equisign.fr>`

1.3. Provide Documentation Feedback

As part of an ongoing process to create documentation that is easy to understand and use, as well as relevant to audience roles as administrator users, we welcome feedback about this guide. Please email any comments or suggestions to: `<support@equisign.fr>`

2. Document Conventions

EquiSign documentation uses typographical conventions with specific meanings. These conventions are described in the following table.

Convention	How It Is Used
bold	Indicates the most important part of a step in step-based instructions. Example: Click the OK button.
italic	Indicates a reference to another document or guide. Example: See the Release Notes. Indicates the name of an access right. Example: The unlock right allows an administrator to help an end user unlock a smart card.

Convention	How It Is Used
`monospaced font`	Indicates a file name, directory name or path, code examples and elements, application output, and user-entered text. Example: Save the file in the `/webserver` directory.
`italicized monospaced font`	Indicates an environment-specific or implementation-specific variable. Example: Save the file in the *`root_directory/`*`webserver` directory.
Important:	Contains important information that must be paid attention to. Failure to do so may have a negative impact on the application.
Note:	Contains valuable supplementary information.
Tip:	Contains helpful information that may be useful, for example, a shortcut or another way of performing a task.

Chapter 1. Installation Architecture Overview

The MFT application is composed of six components: the database, the administration Webapp, the end user Webapp, the Web server, the Network File System, and an optional SMTP connector. These components can be installed using a single-host architecture or a multiple-host architecture. The decision to host the components together or individually is based on load balancing and usage volume considerations.

In multiple-host architectures, the Web server and end user Webapp can both be installed in multiple instances on as many hosts as are necessary to accommodate the file sharing load volume. The administration Webapp can be hosted separately from the Web server and the end user Webapp. The database and the Network File System can also be hosted on dedicated servers. A dedicated Network File System server for remote file storage is rarely necessary.

Before installation, the architecture of the MFT application should be planned in consultation with an assigned Equisign technical representative.

The MFT SMTP Connector is an optional component that receives emails with the SMTP protocol and transforms an SMTP MIME message into an MFT message, which can then be retrieved by its recipients through the MFT end user Webapp. The SMTP Connector is a Mail Delivery Agent (MDA): it does not route the email messages; it only delivers them through MFT. Routing decisions (should this email be delivered using MFT?) are performed by an upstream corporate SMTP server, that is not included in or managed by the MFT platform.

Chapter 2. Install

For security reasons, installation and configuration of Managed File Transfer could be done by an expert from Equisign's Team. On demand, Equisign team could assist on this task and give to specific installation and exploitation guide

To install the Managed File Transfer server application, the installation administrator needs to complete the following tasks:

- Section 2.1, “Prepare for Installation”
- Section 2.2, “Run the Installer”
- Section 2.3, “Complete the Installer Screens”
- Section 2.4, “Initialize the Server Application”

2.1. Prepare for Installation

To prepare for installation, the administrator should complete the following tasks:

1. Prepare the network infrastructure for the server application by opening ports in the firewall, setting firewall input and output rules, and making the DNS server available. Refer to the Managed File Transfer System Maintenance Guide for information about the ports and protocols used by the Managed File Transfer server application.
2. Obtain the installation Base Distribution ISO package from EquiSign.
3. Obtain the lastest MFT service pack from EquiSign.
4. Obtain a license for the host operating system, which must be installed before the Managed File Transfer server application.
5. Obtain the following information which will be requested in the installer screens:
    a. IP addresses/subnet masks, hostnames, and the IP addresses of the DNS servers for servers that have been allocated to host the Managed File Transfer server application, including the public IP address for the Managed File Transfer Web server(s)
    b. IP address or fully-qualified DNS name used to access of the NTP server or servers that will be used to synchronize the time on the host machine
    c. IP address or fully-qualified DNS name used to access the SMTP server that the server application should use to send mail if the default Postfix mail system will not be used
    d. Email addresses for the administrators who should receive system mail from the host machine, primarily from the cron service
6. Obtain the following access rights and permissions:
    a. `root` user access to the machine(s) that will host the server application
7. If not using a certificate signing application, such as a PKI, to sign the Web server certificate during initialization of the Managed File Transfer server application, a pre-purchased Web server certificate that can be integrated with the help of an assigned Equisign technical representative. The minimum encryption strength required for a pre-purchased certificate is 2048 bits.
8. Ensure that an SSH tool is available for logging in to the machine(s) that will host the MFT server application if the installation is being performed remotely.

9. Ensure that all server have access to Internet in order to download required package. In particular on RHEL7/Centos7 must be able to be able to retrieve those yum package

```
yum install dialog postfix ntp perl
yum install epel-release perl-Data-Dumper
yum install NetworkManager-tui
```

2.2. Run the Installer

This section includes instructions on how to use the installation package.

In multi-host environments, the Managed File Transfer installer must be run on each server that will host a Managed File Transfer component. The installer can be run on the host servers in any order.

The Managed File Transfer product-only installer uses the standard RPM package format provided by the host OS distribution to install the product. The resolution of the installation dependencies between EquiSign RPM packages and the required RHEL packages is handled automatically by the yum system.

Procedure 2.1. To run the installer using the installation package containing the Managed File Transfer product on a machine where RHEL has already been installed:

1. Log in to the machine that will host the application server as `root` or another administrator with sufficient privileges to perform the following steps.
2. Make sure the RHEL OS installation and upgrade repositories have been registered using yum.
3. Make sure firewall (iptables, firewalld) are disabled on MFT servers.
4. Make sure SELinux is disabled.
5. To install the prerequisite packages and set up the EPEL package source, enter under CentOS:

   ```
   yum install ntp dialog perl-Data-Dumper epel-release
   ```

   Under Redhat:

   ```
                   cd /tmp
       wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
       sudo yum install epel-release-latest-7.noarch.rpm
       rm epel-release-latest-7.noarch.rpm
                   yum install ntp dialog perl-Data-Dumper
   ```

6. Postfix installation is optional. If postfix is installed, the installer will automatically configure postfix for emails sent by the Managed File Transfer cron jobs. The configuration of a local MTA is required to deliver these emails. If postfix is not installed during this step, make sure that email sent locally to system users `root` and `mft` are sent to the Managed File Transfer administrators.

   To install the postfix package, enter:

   ```
   yum install postfix
   ```

7. To remove sendmail if enabled, enter:

   ```
   yum remove sendmail
   ```

8. Mount the Base Distribution ISO file to any directory on the machine hosting the server application, such as the `/mnt` directory.

   For example, to mount a Base Distribution ISO of the host machine to the `/mnt` directory, enter:

   ```
   mount -t -o loop /path/to/mft.iso  /mnt/
   ```

9. Copy the contents of the EquiSign Managed File Transfer RHEL Base distribution to a directory on the machine that will host the application server, such as the `/tmp` directory. Make sure the administrators who will perform the installation are given write access to the copied files.

10. If not already logged in as `root`, log in to the machine that will host the application server as `root`.

11. To run the Managed File Transfer server application installer, enter:

    ```
    /tmp/opentrust-mft-install
    ```

    where */tmp* is the directory the contents of the Managed File Transfer RHEL Product Base distribution were copied to inStep 9.

12. Continue toSection 2.3, “Complete the Installer Screens”.

2.3. Complete the Installer Screens

EquiSign recommends that Managed File Transfer server application installations be performed on a dedicated, previously unconfigured server. The option to configure the installation properties manually is provided for customers who must follow server policies that conflict with the EquiSign recommendation to use a dedicated, previously unconfigured server. To configure the installation properties manually, read the installer steps and, for each configuration step, edit the same file that the installer writes to.

In multi-host environments, the Managed File Transfer installer screens must be completed on each server that will host a Managed File Transfer component. The installer screens can be run on the host servers in any order.

Procedure 2.2. To run the Managed File Transfer server application installer:

1. On the Hostname and Networking screen, at the "Do you want to configure hostname and networking?" prompt, choose one of the following options:

   - Yes - The option to configure the hostname and networking properties for the OS is provided by bundling configuration screens from the supported OS distributions in the Managed File Transfer server application installer. These screens allow administrators to set the hostname of the machine, set the DNS properties for the machine, configure additional Ethernet cards, add network devices, and set other networking properties. For a previously unconfigured server, the minimum required configurations required to complete the Managed File Transfer server application installer successfully include hostname, DNS, and static IP address configurations. The administrator making these configurations should be familiar with the OS and its related documentation before using these screens. If the administrator performing the installation is not familiar with how to make these configurations, the administrator should contact an assigned Equisign technical representative for help.

   - No - Selecting No will bypass the hostname and networking configuration screens in the Managed File Transfer server application installer. If No is selected and the

required hostname, DNS, and DHCP or static IP address configurations were not made manually before performing the server application installation, the Managed File Transfer installation process cannot be completed successfully.

2. If SSH is being used to access the host machine on which the installation is being performed and changes were made to the hostname and networking configuration, on the Restart Networking screen, at the "Do you want to restart networking in order to use the new settings?" prompt, select one of the following options:

   - Yes - Selecting Yes stops and restarts the networking device and loopback interface of the machine to update them with the new settings.
   - No - If No is selected, the machine can be rebooted manually after running the Managed File Transfer server application installer.

   If SSH is not being used to access the host machine on which the installation is being performed or changes were not made to the hostname and networking configuration, skip this step; the Restart Networking screen will not be displayed.

3. On the NTP Server(s) screen, at the "Please enter one or more NTP server(s) separated by ',"" prompt, enter the IP address or the DNS name used to access the NTP server or servers that will be used to synchronize the time on the host machine. The default NTP servers listed on the NTP Server(s) screen are read from the machine's DHCP information or the default `/etc/ntp.conf` file and server names or IP addresses entered on this screen are written to the `/etc/ntp.conf` file. Multiple NTP servers are allowed for better precision. If multiple NTP servers are entered, the NTP client will recognize all NTP servers as equal. The Managed File Transfer server application installer will attempt to synchronize the clock on the host machine by stopping and re-starting the ntp or ntpd service before continuing to the next installer screen. If the Time Synchronization Failure screen is displayed, correct any errors in the name or IP address entry and verify that the NTP server is operating correctly before selecting Retry.

4. On the Enter SMTP Relay Host screen, at the "Please enter the SMTP relay hostname or IP address" prompt, enter the IP address or the DNS name used to access the SMTP server that the Managed File Transfer server application should use to send system administration email, such as email sent by the cron service. If a server name or IP address is not entered on this screen, the Postfix service will deliver the email without using a relay host. If a server name or IP address is entered on this screen, the server name or IP address is written to the `relayhost = []` parameter in the `/etc/postfix/main.cf` file.

5. On the Configure Email screen, at the "Please enter one or more valid email addresses (separated by ',') where all mail for users root and mft will be redirected or choose Cancel if you want to deal with it manually" prompt, enter the email addresses for the administrators who should receive email notifications for cron events that take place on the host machine, such as Postfix log updates. These email addresses are written to the `/etc/aliases` file. Additions or changes can be made to the list of administrator email addresses after installation by editing the `/etc/aliases` file.

6. If Postfix is not installed, at the "The Postfix MTA is not installed on this system: the installation of the MFT SMTP Connector will not be available. If you wish to install the MFT SMTP Connector, first install the Postfix MTA on this system, then run the install script again." prompt, choose to quit the installer and install Postfix or to continue the installation without the SMTP Connector.

   If Postfix is already installed on the host machine on which the installation is being performed, skip this step; the screen will not be displayed.

7. On the Installation Type screen, at the "Perform a single-host installation?" prompt, choose Yes or No to select the installation type. If No is selected, continue to the next step. If Yes is selected, continue toStep 9.

8. On the Choose Components to Install screen, at the "Choose components to install" prompt, from the following options, select the Managed File Transfer components that will be hosted on the machine on which the installation is being performed:

   - Web Server - for handling end user HTTP requests sent to the end user application
   - End User Webapp
   - Administration Webapp - including its dedicated Web server when the Administration Webapp is not hosted on the same server as the Web Server component
   - Database - the server that will host the database
   - File Server - the server that will be used to host exchanged files
   - SMTP Connector

   All of the Managed File Transfer components, except the SMTP Connector, must be installed. Each component can be installed on its own host machine, all components can be installed on a single host machine, or the components can be logically grouped for installation on multiple host machines. For additional information and recommendations, consult an assigned Equisign technical representative.

9. On the SMTP Connector screen, choose whether to install the SMTP connector if it is covered by the license agreement and enter OK. This screen will only be displayed during single-host installations on machines where Postfix is installed.

10. On the Anti-virus Packages screen, at the "Install ClamAV and enable its use by MFT now?" prompt, select Yes to install the anti-virus packages. This screen will only be displayed when running the installer on a machine that will host an end user Webapp.

11. On the ClamAV Repository screen, note that the repository should be enabled and enter OK. This screen will only be displayed when running the installer on a machine that will host an end user Webapp and will only be displayed if ClamAV is installed using the `opentrust-mft-install` script.

12. On the Installation Complete screen, at the "Do you want to run mft-config now?" prompt, to start the initialization process described inSection 2.4, “Initialize the Server Application”, select Yes and wait for the "Starting mft..." message. If the initialization process should be started later to allow for additional manual configurations on the host machine or initialization of other host machines, select No, review the "OpenTrust MFT has been installed, but not configured. You should run the 'mft-config' script." message, and record the script name for later use. The initialization steps, including running the `mft-config` script, must be performed on the server hosting the Managed File Transfer database component before being performed on other Managed File Transfer host machines.

2.4. Initialize the Server Application

The Managed File Transfer server application initialization process is necessary to prepare the application modules for use and create access rights for an initial configuration administrator. The initialization process contains the following procedures: enabling anti-virus updates in environments that use proxy servers, pre-configuring the application components and modules, handling the application certificate signing requests (CSRs), setting up the Network File System, and starting the application.

To initialize the Managed File Transfer server application for use by administrators, complete the following initialization procedures, in this order:

1. Section 2.4.1, “Enable Anti-virus Updates via Proxy”

2. Section 2.4.2, “Run the Initialization Script for Multi-host and Advanced Single-host Installations ” or Section 2.4.3, “Run the Initialization Script for Simple Single-host Installations”
3. Section 2.4.4, “Configure the Network File System”
4. Section 2.4.5, “Start the Managed File Transfer Application”

2.4.1. Enable Anti-virus Updates via Proxy

Procedure 2.3. To enable regular anti-virus updates, in deployments that use a proxy server:

1. Log into the machine hosting the end user Webapp as the `root` user.
2. To edit the proxy settings configured for the anti-virus configuration to allow automatic updates, open the `/etc/freshclam.conf` file.
3. Add the proxy information needed by the anti-virus configuration in the Proxy Settings section of the file.

2.4.2. Run the Initialization Script for Multi-host and Advanced Single-host Installations

In multi-host environments, this procedure must be performed on the servers hosting Managed File Transfer components in this order:

1. the server hosting the database
2. the server hosting the administration Webapp
3. the server hosting the end user Webapp(s)
4. the server hosting the Web server(s)

The initialization script cannot be run on a server hosting only the Network File System component, as there is no pre-configuration required for the Network File System component.

Procedure 2.4. To run the advanced single-host/multi-host initialization script and pre-configure the application components and modules:

1. If the `mft-config` script is not being run from the option at the end of the installer screen steps:
   a. Log in to the server hosting the Managed File Transfer server application as the `root` user.
   b. To start the initialization script, enter:

```
/opt/opentrust/mft/sbin/mft-config
```

   c. On the "Install a Simple Configuration?" screen, click No to use the initialization process appropriate for multi-host installations and advanced single-host installations. This option will only be displayed if all of the Managed File Transfer components are installed on the server being initialized. If Yes is selected to be able to common

values as defaults for some of the configurations in a single-host installation, follow the instructions inSection 2.4.3, “Run the Initialization Script for Simple Single-host Installations”.

If the `mft-config` script is being run from the option at the end of the installer screen steps, skip this step, as the "Install a Simple Configuration?" screen will not be displayed.

2. On the "Please Choose a Component to Initialize" screen, verify that all of the components hosted on the server being initialized, as selected inStep 8, are displayed on the screen, select a component to initialize, and click OK.

   All of the components displayed on the screen must be initialized. Follow the instructions that correspond to each component:

   - Step 3 - Database Server
   - Step 4 - Bootstrap
   - Step 5 - Application Server (Webapps)
   - Step 6 - Web Server; when the Web server component is not hosted on the same server as the administration Webapp application server, these steps must be performed on both the Web server component and the administration Webapp application server component to accommodate the embedded Web server for the administration Webapp application server.
   - Step 7 - SMTP Connector

3. If the Database Server component was selected to be initialized:

   a. On the Database Server Initialization screen, select Database Access and click OK.

   b. On the Enter Password screen, enter a password to be used for database access and click OK.

   c. On the Confirm Password screen, re-enter the password and click OK.

   d. On the Enter Authorized Subnetwork screen, enter the subnets authorized to access the database or leave the field blank to authorize all subnets to access the database and click OK.

   e. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

   f. After being returned to the Database Server Initialization screen, to return to the "Please Choose a Component to Initialize" screen, click Back.

4. If the Bootstrap Configuration component was selected to be initialized:

   a. On the Public Server Name screen, enter the DNS name of the server that end users will use to access the end user Webapp and then click OK. The DNS name will be used to create the URL used to access the end user Webapp. In multi-host installations, this DNS name will not be the DNS name of the server hosting the end user Webapp component. The DNS name corresponds to the URL used to connect to the Web server used by the end user Webapp.

   b. If an SMTP Relay Hostname screen is displayed, enter the IP address or the DNS name used to access the SMTP relay server host.

   c. On the Application Administrator's Email Address screen, enter a "from" address for email that will be sent to administrators who receive notifications from the server

application, such as administrators who are notified when end users request quota increases. Then click OK.

d. On the System Administrator's Email Address screen, enter an email address to which email for users "root" and "mft" will be redirected and for the administrators who should receive email notifications for cron events that take place on the host machine, such as Postfix log updates. These email addresses are written to the `/etc/aliases` file. Additions or changes can be made to the list of administrator email addresses after installation by editing the `/etc/aliases` file. Then click OK.

e. On the Reply-to/Sender's Email Address screen, enter the email address to be used for sending email to application and system administrators.

f. On the Activate Anti-virus screen, accept the default of Disabled to choose not to use the bundled ClamAV antivirus protection or choose CLAMD to enable the bundled ClamAV anti-virus protection. Then click OK.

g. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

5. If an Application Server (Webapps) component was selected to be initialized, each displayed sub-component must be initialized:

   - Administration Webapp -Step 5.a, only displayed on servers hosting the administration Webapp
   - End User Webapp -Step 5.b, only displayed on servers hosting an end user Webapp
   - Licensing - Step 5.c
   - Logs Signing -Step 5.d, optional, only displayed on servers hosting the administration Webapp
   - Database Access - Step 5.e

   a. On the Webapps Initialization screen, select Administration Webapp, if available, and click OK.

      i. On the Enter Description screen, enter a description for the administration Webapp. The description entered will not be displayed in the application. Then click OK.

      ii. On the Enter Hostname screen, enter the DNS name used to access the server hosting the administration Webapp, which can be used by other Webapps to access the administration Webapp, and click OK.

      iii. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

   b. After being returned to the Webapps Initialization screen, select End User Webapp, if available, and click OK.

      i. On the Enter Identifier screen, enter an identifier for the end user Webapp or accept the default of `user`. The identifier entered must match the identifier entered in Step 6.b.i; the common identifier enables session affinity and load-balancing. Then click OK.

      Session affinity works as follows: when a user connects to a Web server user interface for the first time, the request is forwarded to an application server (a Webapp) among the application server pool. A user session is created on the

application server. Session affinity ensures that subsequent user requests will always be forwarded by the Web server to the same application server where the user session has been initially created. Each end user Webapp possesses its own identifier and each identifier is referenced by the user interface Web server so that it can forward user requests to the appropriate Webapp.

ii. On the Enter Description screen, enter a description for the end user Webapp. The description entered will not be displayed in the application. Then click OK.

iii. On the Enter Hostname screen, enter the DNS name used to access the server hosting the end user Webapp, which can be used by other Webapps to access the end user Webapp, and click OK.

iv. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

c. After being returned to the Webapps Initialization screen, select Licensing, if available, and click OK.

i. If a License Server Proxy screen is displayed while initializing the server hosting the administration Webapp, choose whether to configure a proxy to be used by the Managed File Transfer application's licensing server to access a certified time source. Then click OK.

Note

For additional information regarding proxy configuration, refer to the MFT 2.5 Proxy Configuration Tech-Note which can be obtained from an assigned Equisign technical representative.

---

ii. If the choice was to configure a proxy, on the Proxy DNS Name screen, enter the proxy to be used. Then click OK.

iii. If the choice was to configure a proxy, on the Proxy Port screen, enter the port to be used. Then click OK.

iv. If a License Server Access screen is displayed while initializing the server hosting the end user Webapp, enter the DNS name used to access the server hosting the administration Webapp. Then click OK.

v. If a Summary screen is displayed, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

d. After being returned to the Webapps Initialization screen, select Logs Signing, if available, and click OK. The logs signing initialization steps are optional and should only be performed if the application logs should be signed.

i. On the Logs Signing screen, choose a method for registering the certificate to be used to sign the logs:

- Create Certificate Private Key - Step 5.d.ii
- Import Certificate Private Key - Step 5.d.iii
- Import PKCS12 - Step 5.d.iv

ii. If the choice is to generate a private key, on the Logs Signing screen, to begin the process of creating a private key for the log module's certificate, select Create Certificate Private Key and then click OK.

A. On the Choose Key Size screen, choose the encryption strength to use for the private key and click OK.

B. On the Export CSR and Import Signed Certificate or Generate Self-signed Certificate screen, choose a signing method and follow the instructions in the appropriate substep.

I. If the choice is to export the CSR to have it signed and then import the signed certificate:

1. Select Export Certificate Signing Request and click OK.

2. On the Select Directory screen, enter the directory path, without the file name, to the location the CSR should be exported to or accept the default selection of the `/tmp` directory and click OK.

3. On the CSR Exported screen, review the "The CSR has been exported as..." message containing the CSR file name and location and click OK.

4. Leave the initialization procedure for the server currently being initialized, without closing the session, and use another application to sign the CSR. To use a pre-purchased Web server certificate instead of having using the exported CSR, contact an assigned Equisign technical representative for more information.

5. When a signed certificate has been obtained, return to the Export CSR and Import Signed Certificate or Generate Self-signed Certificate screen in the initialization procedure, select Import Signed Certificate and click OK.

6. On the Enter Directory and File Name screen, enter the directory path location and file name for the signed certificate and click OK. The certificate must be in PEM format.

7. On the Import Successful screen, click OK.

8. On the Manage Web Server Certificate screen, to return to the Web Server Initialization screen, click Back.

II. If the choice is to generate a self-signed certificate:

1. Select Generate Self-signed Certificate and click OK.

2. On the Generation and Import Success screen, at the "The self-signed certificate has been generated and imported." prompt, click OK.

iii. If the choice is to import a private key before creating a certificate, on the Logs Signing screen, to begin the process, select Import Certificate Private Key and click OK.

For help with this process, contact an assigned Equisign technical representative.

iv. If the choice is to import a PKCS12 instead of importing or generating a private key, on the Logs Signing screen, select Import PKCS12 and then click OK.

A. On the PKCS12 Filename screen, enter the filepath and filename of a PKCS12 file that has been copied to a directory on the server being initialized. Then click OK.

B. On the PKCS12 Password screen, enter the password of the PKCS12 file that is being imported. Then click OK.

C. On the Success screen, at the "The private key and certificate have been imported." success message, click OK.

v. After being returned to the Logs Signing screen, to return to the Webapps Initialization screen, click Back.

e. After being returned to the Webapps Initialization screen, select Database Access and click OK.

i. If a Database Host screen is displayed, enter the DNS name or IP address used to access the server hosting the database component and click OK.

ii. On the Database Password screen: For multi-host installations, enter the database password that was configured inStep 3.b. For single-host installations, enter a database password and click OK.

iii. On the Confirm Password screen, re-enter the database password and click OK.

iv. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

f. After being returned to the Webapps Initialization screen, to return to the "Please Choose a Component to Initialize" screen, click Back.

6. If the Web Server component was selected to be initialized, each displayed sub-component must be initialized:

- General - Step 6.a
- Add End User Webapp Connection - Step 6.b
- Set Admin Webapp Connection - Step 6.c
- Manage Web Server Certificate - Step 6.d

a. On the Web Server Initialization screen, select General and click OK.

i. On the Enter DNS Name screen, enter the DNS name that will be used to access the server hosting the Web server and click OK. When completing these steps for the embedded Web server of the administration Webapp, the DNS name entered should be the DNS name of the server hosting the administration Webapp component, not the server hosting the Web server component. Then click OK.

ii. On the Client SSL Authentication Type screen, select the type of authentication to use for administrators and end users who connect to the Managed File Transfer user interfaces:

- None - No SSL authentication will be required; select this option if x509 client certificate authentication will not be implemented
- Optional - SSL authentication will be optional; select this option if authentication using x509 client certificates will be implemented

- Require - SSL authentication will be required; this option should not be selected for most deployments

and then click OK.

iii. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

b. After being returned to the Web Server Initialization screen, select Add End User Webapp Connection and click OK.

i. On the Enter Identifier screen, enter the end user Webapp identifier. The identifier entered must match the identifier entered inStep 5.b.i, so that "session affinity" and load-balancing are enabled. Then click OK.

Session affinity works as follows: when a user connects to a Web server user interface for the first time, the request is forwarded to an application server (a Webapp) among the application server pool. A user session is created on the application server. Session affinity ensures that subsequent user requests will always be forwarded by the Web server to the same application server where the user session has been initially created. Each end user Webapp possesses its own identifier, and each identifier is referenced by the user interface Web server so that it can forward user requests to the appropriate Webapp.

ii. On the Enter Hostname or IP Address screen, enter the DNS name or the IP address used to access the server hosting the end user Webapp and then click OK.

iii. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

c. After being returned to the Web Server Initialization screen, select Set Admin Webapp Connection and click OK.

i. On the Enter Hostname or IP Address screen, enter the DNS name or the IP address used to access the server hosting the administration Webapp and then click OK.

ii. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

d. After being returned to the Web Server Initialization screen, select Manage Web Server Certificate and click OK.

e. On the Manage Web Server Certificate screen, choose a method for registering the certificate to be used for the Web server:

- Create Certificate Private Key - Step 6.e.i
- Import Certificate Private Key - Step 6.e.ii
- Import PKCS12 - Step 6.e.iii

i. If the choice is to generate a private key, on the Manage Web Server Certificate screen, to begin the process of creating a private key for the Web server's certificate, select Create Certificate Private Key and then click OK.

A. On the Choose Key Size screen, choose the encryption strength to use for the private key and click OK.

B. On the Export CSR and Import Signed Certificate or Generate Self-signed Certificate screen, choose a signing method and follow the instructions in the appropriate substep.

I. If the choice is to export the CSR to have it signed and then import the signed certificate:

1. Select Export Certificate Signing Request and click OK.

2. On the Select Directory screen, enter the directory path, without the file name, to the location the CSR should be exported to or accept the default selection of the `/tmp` directory and click OK.

3. On the CSR Exported screen, review the "The CSR has been exported as..." message containing the CSR file name and location and click OK.

4. Leave the initialization procedure for the server currently being initialized, without closing the session, and use another application to sign the CSR. To use a pre-purchased Web server certificate instead of having using the exported CSR, contact an assigned Equisign technical representative for more information.

5. When a signed certificate has been obtained, return to the Export CSR and Import Signed Certificate or Generate Self-signed Certificate screen in the initialization procedure, select Import Signed Certificate and click OK.

6. On the Enter Directory and File Name screen, enter the directory path location and file name for the signed certificate and click OK. The certificate must be in PEM format.

7. On the Import Successful screen, click OK.

8. On the Manage Web Server Certificate screen, to return to the Web Server Initialization screen, click Back.

II. If the choice is to generate a self-signed certificate:

1. Select Generate Self-signed Certificate and click OK.

2. On the Generation and Import Success screen, at the "The self-signed certificate has been generated and imported." prompt, click OK.

ii. If the choice is to import a private key before creating a certificate, on the Web Server Certificate screen, to begin the process, select Import Certificate Private Key and click OK.

- On the Private Key Filename screen, enter the filepath and filename of the private key that has been copied to a directory on the server being initialized. The private key must be in PEM format without password protection. Then click OK.

  The Web server's certificate chain file (the issuing CA's certificate and the intermediate CA's certificates up to a root CA) can also be imported as a bundle. The Web server's certificate chain is made available to HTTPS clients to verify the Web server's certificate, up to one of their trusted root CAs. The

Web server's certificate chain file is usually provided by the CA that generated the Web server's certificate. For example, the chain is one of the attachments in the default email templates for delivering a server certificate in PKI.

For help with this process, contact an assigned Equisign technical representative.

iii. If the choice is to import a PKCS12 instead of importing or generating a private key, on the Web Server Certificate screen, select Import PKCS12 and then click OK.

A. On the PKCS12 Filename screen, enter the filepath and filename of a PKCS12 file that has been copied to a directory on the server being initialized. Then click OK.

B. On the PKCS12 Password screen, enter the password of the PKCS12 file that is being imported. Then click OK.

C. On the Success screen, at the "The private key and certificate have been imported." success message, click OK.

iv. After being returned to the Manage Web Server Certificate screen, to return to the Webapps Initialization screen, click OK.

f. After being returned to the Web Server Initialization screen, to return to the "Please Choose a Component to Initialize" screen, click Back.

7. If the SMTP Connector component was selected to be initialized, each displayed sub-component must be initialized:

- Connection to MFT - Step 7.a
- Authentication to MFT - Step 7.b
- SMTP Connector Behavior - Step 7.c
- SMTP Connector Options - Step 7.d

a. On the SMTP Connector Initialization screen, select Connection to MFT and click OK.

i. On the SMTP Connector Access Configuration screen, enter the DNS name that will be used to access the end user Webapp. Then click OK.

ii. On the next screen, enter the network/netmask patterns that will be allowed to relay mail through the SMTP Connector and then click OK. For example, a typical value would be "168.100.189.0/28" when a company's Microsoft Exchange Server belongs to the 168.100.189.0 subnet.

iii. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

b. After being returned to the SMTP Connector Initialization screen, select Authentication to MFT and then click OK.

i. On the next screen, enter the UID of a user account that will be created specifically for using the SMTP Connector and then click OK. This user is used to send messages on behalf of email senders, so it should be either a group impersonator to send messages on behalf of a group of users or have the global Impersonation right to send messages on behalf of any user.

ii. On the next screen, enter the password of the user account that will be created and used to send messages on behalf of email senders and then click OK.

iii. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

c. After being returned to the SMTP Connector Initialization screen, select SMTP Connector Behavior and then click OK.

The "pass-through" option available for the following sub-steps relays the email "as is" via the SMTP Connector to its final recipients, without processing by MFT.

i. Choose one of the options for how to handle S/MIME signed email and then click OK.

ii. Choose one of the options for how to handle S/MIME encrypted email and then click OK.

iii. Choose one of the options for how to handle email without attachments and then click OK.

iv. Choose one of the options for how to handle email that cannot be parsed correctly and then click OK.

v. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

d. After being returned to the SMTP Connector Initialization screen, select SMTP Connector Options and click OK.

i. Enter the return path to be used by the connector when sending emails and then click OK.

ii. Enter the language abbreviations for the languages that should be included in error emails and then click OK.

iii. Enter the minimum email size for emails to be sent to MFT and then click OK.

iv. Enter the maximum email size for emails to be sent to MFT and then click OK.

v. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

e. After being returned to the SMTP Connector Initialization screen, to return to the "Please Choose a Component to Initialize" screen, click Back.

8. When all components listed on the "Please Choose a Component to Initialize" screen have been initialized, click Exit.

2.4.3. Run the Initialization Script for Simple Single-host Installations

Procedure 2.5. To run the simplified initialization script and pre-configure the application components and modules in single-host environments:

1. If the `mft-config` script is not being run from the option at the end of the installer screen steps:

   a. Log in to the server hosting the Managed File Transfer server application as the `root` user.

   b. To start the initialization script, enter:

   ```
   /opt/opentrust/mft/sbin/mft-config
   ```

   c. On the "Install a Simple Configuration?" screen, click Yes to use a simplified initialization process appropriate for most single-host installations. This option will only be displayed if all of the Managed File Transfer components are installed on the server being initialized. If No is selected to be able to make additional initialization configurations to a single-host installation, such those related to the database server, follow the instructions inSection 2.4.2, “Run the Initialization Script for Multi-host and Advanced Single-host Installations ”.

   If the `mft-config` script is being run from the option at the end of the installer screen steps, skip this step, as the "Install a Simple Configuration?" screen will not be displayed.

2. On the "Please Choose a Component to Initialize" screen, select a component to initialize, and click OK.

   All of the components displayed on the screen must be initialized. Follow the instructions that correspond to each component:

   - Bootstrap Configuration - The instructions for initializing the Bootstrap application server component are explained inStep 3.
   - Web Server - The instructions for initializing the Web Server component are explained inStep 5.
   - Application Server - The instructions for initializing the Webapps component are explained inStep 4.
   - SMTP Connector - The instructions for initializing the SMTP Connector component are explained inStep 6.

3. If the Bootstrap Configuration application server component was selected to be initialized:

   a. On the Public Server Name screen, enter the DNS name of the server that end users will use to access the end user Webapp and then click OK. The DNS name will be used to create the URL used to access the end user Webapp. The DNS name corresponds to the URL used to connect to the Web server used by the end user Webapp.

   b. On the SMTP Relay Host screen, enter the DNS name used to access the SMTP relay host. Then click OK.

   c. On the Application Administrator's Email Address screen, enter a "from" address for email that will be sent to administrators who receive notifications from the server application, such as administrators who are notified when end users request quota increases. Then click OK.

d. On the System Administrator's Email Address screen, enter an email address to which email for users "root" and "mft" will be redirected and for the administrators who should receive email notifications for cron events that take place on the host machine, such as Postfix log updates. These email addresses are written to the `/etc/aliases` file. Additions or changes can be made to the list of administrator email addresses after installation by editing the `/etc/aliases` file. Then click OK.

e. On the Reply-to/Sender's Email Address screen, enter the email address to be used for sending email to application and system administrators.

f. On the Summary screen, at the "Is this configuration OK?" prompt, review the summary information and click Yes to continue or No to return to the previous screens.

4. If the Application Server (Webapps) component was selected to be initialized, each displayed sub-component must be initialized:

   - Licensing - The instructions for initializing the General sub-component are explained in???.
   - Logs Signing - The instructions for initializing the Logs Signing sub-component are explained inStep 5.d.
   - Database Access - The instructions for initializing the Database Access sub-component are explained inStep 5.e.

5. If the Web Server component was selected to be initialized, each displayed sub-component must be initialized:

   - General - The instructions for initializing the General sub-component are explained inStep 6.a.
   - Manage Web Server Certificate - The instructions for initializing the Manage Web Server sub-component are explained inStep 6.d.

6. If the SMTP Connector component was selected to be initialized, each displayed sub-component must be initialized:

   - Connection to MFT - The instructions for initializing the connection to MFT are explained inStep 7.a.
   - SMTP Connector Behavior - The instructions for initializing SMTP Connector behavior are explained inStep 7.c.
   - SMTP Connector Options - The instructions for initializing SMTP Connector options are explained inStep 7.d.

7. When all components listed on the "Please Choose a Component to Initialize" screen have been initialized, click Exit.

2.4.4. Configure the Network File System

This procedure is not required if the administration and end user Webapps are hosted on the same server as the server hosting the file server component, as there is no need to access the exchanged files remotely. If the Webapps and File Server component are not hosted on the same servers, this procedure must be performed on each server hosting a Webapp or the file server component.

The `nfs-utils` and `portmap` or `rpcbind` (according to the corresponding host OS) packages must be installed on the Webapp and File Server component host servers before performing the steps in this section.

Procedure 2.6. To configure the Network File System for the Managed File Transfer server application:

1. Log in to the server hosting the Managed File Transfer file server component as the `root` user.
2. To start the Network File System services, enter the command that corresponds to the host OS:
   - On RHEL 5:

     ```
     service portmap start
     ```

   - On RHEL 6:

     ```
     service rpcbind start
     ```

   - On RHEL 7/Cento7:

     ```
     systemctl start rpcbind
     ```

   and then enter:

   - On RHEL 5/ RHEL 6:

     ```
     service portmap start
     ```

   - On RHEL 7/Cento7:

     ```
     systemctl start nfs
     ```

3. To declare each Webapp host machine, enter:

   ```
   /opt/opentrust/mft/sbin/nfs-management config --add
                            fqdn_of_server_hosting_End_User_Web_application
                            /opt/opentrust/mft/sbin/nfs-management config --add
                            fqdn_of_server_hosting_Administration_Web_
                                application
   ```

   where the *`fqdn_of_host_server`* is the fully-qualified DNS name used to access each host server.
4. To save the modifications, enter:

   ```
   /opt/opentrust/mft/sbin/nfs-management config --exportfs
   ```

5. To enable Network File System startup when the server boots, enter:

   ```
   chkconfig nfs on
   ```

   and then enter the command that corresponds to the host OS:

   - On RHEL 5:

     ```
     chkconfig portmap on
     ```

   - On RHEL 6:

     ```
     chkconfig rpcbind on
     ```

   - On RHEL 7/Cento7:

     ```
     systemctl enable rpcbind
                               systemctl enable nfs-server
     ```

6. Log in to the server hosting the Managed File Transfer Administration Webapp component as the `root` user.

7. To declare the Network File System host server, enter:

```
/opt/opentrust/mft/sbin/nfs-management config --server
                            fqdn_of_server_hosting_File_Server_component
```

8. To start the Portmap service, enter the command that corresponds to the host OS:

   - On RHEL 5:

```
service portmap start
                                        chkconfig portmap on
```

   - On RHEL 6:

```
service rpcbind start
                                        chkconfig rpcbind on
```

   - On RHEL 7/Cento7:

```
systemctl start rpcbind
```

9. To mount the Managed File Transfer server application to the Network File System, enter:

```
/opt/opentrust/mft/sbin/nfs-management mount
```

10. Log in to the server(s) hosting the Managed File Transfer End User Webapp component(s) as the `root` user and repeat Step 7 throughStep 9.

2.4.5. Start the Managed File Transfer Application

The Managed File Transfer server application must be started on each server hosting Managed File Transfer server application components, except for servers hosting only the File Server component. In multi-host environments, the Managed File Transfer server application should be started on the host servers in this order:

1. server hosting the database component
2. server hosting the administration Webapp component
3. server hosting the end user Webapp component
4. server hosting the Web server application component

Procedure 2.7. To start the Managed File Transfer server application:

1. Log in to the server hosting the Managed File Transfer server application as the `root` user.
2. Enter:

```
service mft start
```

   When the Managed File Transfer service is started on a server hosting the administration Webapp, an initial administrator for the Managed File Transfer server application is created automatically, with username `admin-mft` and default password `opentrust`.

3. Notify the Managed File Transfer server application administrator that the Managed File Transfer server application is ready to be configured using the instructions in the Managed File Transfer Server Configuration Guide.

   The URL to access the administration Webapp is: `https://dnsnameofhost/mft` , where *`dnsnameofhost`* is the DNS name used to access the server hosting the administration Webapp component.

   The URL to access the end user Webapp is `https:// dnsnameofhost` , where *`dnsnameofhost`* is the DNS name that was entered to access the End User Webapp for multi-host installations and is the DNS name of the server hosting all of the Managed File Transfer components for single-host installations. The URL used to access the end user Webapp is always based on the DNS name used to access the server hosting the Apache Web server application component, to allow for "n" number of load-balanced end user Webapp host servers that all use a single interface.

   The initial administrator can log in using `admin-mft` as the username and `opentrust` as the password.

2.5. Installation of the service pack

MFT Service pack will install the fix and new functionnalities and must be applied.

As a requirement, the /tmp of every server must be able to contain executable script.

Procedure 2.8. To install service pack:

1. Log in to the server hosting the Managed File Transfer server application, Managed File Transfer web front and Managed File Transfer database server as the `root`user.
2. run a service mft stop in order to stop all the MFT daemon
3. copy the service pack on each machine in the /tmp directory
4. unzip the service pack and run in the service pack directory.
5. run chmod +x /tmp/mft_service_pack/install.sh
6. run the install script by running in root /tmp/mft_service_pack/install.sh
7. After applying the install script on each server, run a service mft start in order to start all the MFT daemon

Chapter 3. Upgrade

For security reasons, configuration of new features of Managed File Transfer could be done by an expert from Equisign's Team. On demand, Equisign team could assist on this task and give to specific upgrade and exploitation guide

There are two types of upgrades for the Managed File Transfer server application:

- Maintenance Upgrades - Maintenance upgrades include new versions or patches for OS distribution files and third-party software files used by the Managed File Transfer application. These upgrades are the responsibility of the customer and should be performed regularly. The customer needs to obtain all necessary OS upgrade files and licenses directly from the host OS distribution. The customer needs to obtain all necessary third-party software file upgrades and licenses directly from the third-party software providers, except in the case of security alerts for third-party software bundled with theManaged File Transferserver application, which will be supported by a new product release from EquiSign. Review the Section 3.1, “EquiSign Maintenance Upgrade Policy” for more information.

- Product Release Upgrades - EquiSign product release upgrades include new features or enhancements for Managed File Transfer and are versioned by release number. EquiSign recommends upgrading to the latest version ofManaged File Transferwhen new major versions are released and applying patches or maintenance releases when necessary, as indicated by the EquiSign Support Team.

  Before performing maintenance or product release upgrades, review the Section 3.1, “EquiSign Maintenance Upgrade Policy” and Section 3.3, “Upgrade to the 3.3.6.4 Product Release or Update Server Application” .

3.1. EquiSign Maintenance Upgrade Policy

3.1.1. Overview of Files to Be Maintained

The installation and upgrade packages could be obtained on demand from `https://support.equisign.fr/`, after creating a support ticket. Then Equisign will send to you Managed File Transfer that will have the given format:

- The Base Distribution of Managed File Transfer in ISO file format (Base Installation)

- The last service pack of Managed File Transfer in zip file format (Enhancements and security fixes)

3.1.2. Customer Responsibilities

For all installations, it is the responsibility of the customer to ensure that the host OS is legally licensed, to maintain and upgrade the host OS by obtaining and applying all patches and upgrades whenever patches and upgrades are made available by the host OS distribution. It is the responsibility of the Managed File Transfer customer to ensure that the host OS is supported by EquiSign.

3.1.3. Security Patches

Security patches for the host OS distribution should be applied before installing or upgradingManaged File Transfer. In cases where the customer uses the bundled host OS Managed File Transfer installation package, EquiSign strongly recommends applying security patches for the host OS distribution immediately after installingManaged File Transfer. For all Managed File Transfer installations, with and without the bundled host OS, the EquiSign Support Team may require a customer to apply host OS distribution upgrades or downgrades and security patches to resolve issues with the customer's product installation or before performing an upgrade to the latest product release ofManaged File Transfer.

3.1.4. EquiSign Support for Third-party RPM Packages Included in EquiSign Installation Packages

All Managed File Transfer installation packages, with without the bundled host OS, contain Managed File Transfer application files and third-party RPM packages required byManaged File Transfer. EquiSign will support the third-party files that are included in the Managed File Transfer installation packages by providing product releases for Managed File Transfer when the included third-party files are subject to security alerts. For OS files that are not yet part of the host OS distribution or that were patched by EquiSign (e.g., mod_ssl), EquiSign will upgrade the software at the same pace as the host OS distribution.

Note

Use of the third-party software included in the Managed File Transfer installation packages for any use other than the proper functioning of an EquiSign product is not supported by EquiSign.

3.2. Upgrade to the lastest Product Release from 3.3.6.4 release

After reading Section 3.2.1, “Supported Upgrade Paths” and the Managed File Transfer Release Notes , upgrade administrators should follow the upgrade instructions found in:

- Section 3.2.2, “Upgrade Server Application, Add New Components or Features, or Change System Settings”

The Managed File Transfer server application upgrade will require the upgrade of system RPM packages.

3.2.1. Supported Upgrade Paths

EquiSign supports the following upgrade paths forManaged File Transfer:

- 3.3.6.4 and higher to 3.4.0.0

To upgrade from an earlier version of the product, please follow the upgrade to 3.3.6.4 in Section 3.3, “Upgrade to the 3.3.6.4 Product Release or Update Server Application”

3.2.2. Upgrade Server Application, Add New Components or Features, or Change System Settings

This procedure must be performed on all servers hosting Managed File Transfer components, in the following order:

1. the server hosting the database
2. the server hosting the administration Webapp
3. the server hosting the end user Webapp(s)
4. the server hosting the Web server(s)

As a requirement, the /tmp of every server must be able to contain executable script.

To upgrade the Managed File Transfer server application, add new components or features, or change system settings:

1. If not already logged in as the `root` user, log in to the machine hosting the Managed File Transfer component or components as the **`root`** user.
2. Log in to the EquiSign Support Site and create a ticket to demand the last service pack zip file.
3. Then, we communicate to you the release note and the last service pack zip file so that you can make the upgrade
4. Unzip the service pack to /tmp on all the machine hosting theManaged File Transfer.
5. Verify that all MFT server has access to Internet
6. Verify that the appropriate repositories are configured for the OS: Make sure the following yum repositories have been registered:

   - the RHEL/CentOS OS installation repository
   - the RHEL/CentOS OS upgrade repository (the latest version of the OS with the same major version number)

   These OS repositories must be configured or the upgrade process may fail due to missing required packages.
7. Log in to the server hosting the Managed File Transfer server application, Managed File Transfer web front and Managed File Transfer database server as the `root`user.
8. run a service mft stop in order to stop all the MFT daemon
9. copy the service pack on each machine in the /tmp directory
10. extract the installation files from the autoextractable script by running : /tmp/mft-servicepack-<version>-r<revision>.sh
11. run the installer as instructed by the autoextractable script : /tmp/mft_installer_XXXX/install_mft.sh
12. restart MFT by running : service mft restart

3.3. Upgrade to the 3.3.6.4 Product Release or Update Server Application

After reading Section 3.3.1, "Supported Upgrade Paths" and the Managed File Transfer Release Notes , upgrade administrators should follow the upgrade instructions found in:

- Section 3.3.2, "Upgrade Server Application, Add New Components or Features, or Change System Settings"

The Managed File Transfer server application upgrade will require the upgrade of system RPM packages.

3.3.1. Supported Upgrade Paths

EquiSign supports the following upgrade paths forManaged File Transfer:

- 2.0 and higher to 3.3.6.4

To upgrade from an earlier version of the product, contact an assigned Equisign technical representative.

3.3.2. Upgrade Server Application, Add New Components or Features, or Change System Settings

This procedure must be performed on all servers hosting Managed File Transfer components, in the following order:

1. the server hosting the database
2. the server hosting the administration Webapp
3. the server hosting the end user Webapp(s)
4. the server hosting the Web server(s)

Procedure 3.1. To upgrade the Managed File Transfer server application, add new components or features, or change system settings:

1. If not already logged in as the `root` user, log in to the machine hosting the Managed File Transfer component or components as the **`root`** user.
2. Log in to the EquiSign Support Site and create a ticket to demand the Base Distribution 3.3.6.4 iso file.
3. Then, we communicate to you the release note and the Base Distribution 3.3.6.4 iso file so that you can install it
4. Mount the Base Distribution ISO to any directory on the machine hosting the Managed File Transfer server application, such as the `/mnt` directory.

   For example, to mount a Base Distribution ISO to the `/mnt` directory, enter:

```
mount -t -o loop /path/to/mft.iso /mnt/
```

5. Verify that the appropriate repositories are configured for the OS: Make sure the following yum repositories have been registered:

   - the RHEL/CentOS OS installation repository
   - the RHEL/CentOS OS upgrade repository (the latest version of the OS with the same major version number)

   These OS repositories must be configured or the upgrade process may fail due to missing required packages. The Managed File Transfer upgrader will only install or upgrade OS packages that are strictly required by the RPM packages. Other OS packages will not be upgraded.

6. To change to the directory where the Base Distribution ISO was mounted, enter:

   ```
   cd /
                              directory
   ```

   where *`directory`* is the name of the directory to which the Base Distribution ISO was mounted inStep 4, such as the `/mnt` directory.

7. This step must be performed on all servers hosting Managed File Transfer components.

   To run the Managed File Transfer upgrader, enter:

   ```
   ./opentrust/opentrust-mft-upgrade
   ```

   with the opentrust directory only being included in the command path for upgrades using the Base Distribution ISO. The Managed File Transfer upgrader will stop the `mft` service.

   a. In the automated upgrader, if an MFT Upgrade screen is displayed because the upgrade script is being run for the first time on a server hosting an earlier version of the product, at the "Do you want to continue?" prompt, select Yes.

   b. For upgrades from versions earlier than 2.5, choose the upgrade steps that correspond to the Managed File Transfer host server:

      - When running the upgrader on a server that does not host the administration Webapp or an end user Webapp, continue toStep 7.j.
      - When running the upgrader on the server hosting the administration Webapp or an end user Webapp, on the "Do You Want to Run `mft-config` Now?" screen, select Yes.

      For upgrades from versions 2.5 and later, continue toStep 7.j.

   c. On the "Please Choose an Item to Configure" screen, select Webapps and click OK.

   d. On the Webapps Configuration screen, select Licensing and click OK.

      i. When running the upgrader on the server hosting the administration Webapp, on the License Server Proxy Configuration screen, choose whether to configure a proxy connection to be used by the internal licensing time service:

         - Yes - On the Enter Proxy DNS Name screen, enter the DNS name used to access the proxy server and click OK. On the Enter Proxy Port screen, enter the port number to access on the proxy server and click OK.
         - No - Continue to the next step.

ii. When running the upgrader on a server hosting an end user Webapp, on the Network License Server Access Configuration screen, enter the DNS name used to access the server hosting the administration Webapp and click OK.

e. On the "Is this configuration OK?" screen, select Yes.

f. On the Webapps Configuration screen, click Back.

g. On the "Please Choose an Item to Configure" screen, click Exit. Continue to Step 8.

h. If upgrading from a version earlier than 2.6, at the "Would you like to zone the logs currently on your platform?" prompt, select Yes to launch the zone-logs script or No to launch the `/opt/opentrust/mft/sbin/zone-logs` script at a later time using `/opt/opentrust/mft/sbin/zone-logs`.

i. When the System Configuration screen is displayed again, repeat Step 7.g until the choice is to quit the upgrade script.

j. On the Upgrade Success screen, at the "Do you want to restart MFT now?" prompt, select one of the following options:

- To start the Managed File Transfer server application now, select Yes.
- If the Managed File Transfer server application should be started later to allow for additional manual configurations on the host machine, select No and note that the Managed File Transfer server application can be started later by running `/etc/init.d/mft start` or rebooting the computer to automatically restart the server application.

The restart prompt screen may not be displayed when running the upgrader on servers hosting the administration Webapp or an end user Webapp or when scripts external to the installation script have been launched from the installation script.

8. If the Managed File Transfer server application was not restarted using the automated upgrader, this step must be performed.

   To restart the Managed File Transfer server application and complete the upgrade process, enter:

```
service mft start verbose
```

9. To unmount the Base Distribution ISO, enter:

```
cd /
                          umount /
                          directory
```

   where *`directory`* is the name of the directory to which the Base Distribution ISO was mounted inStep 4, such as the `/mnt` directory.

10. View the upgrade log file in the `/opt/opentrust/var/log` directory.

11. To configure the product license, refer to the instructions in theManaged File Transfer Server Configuration Guide.

3.4. Upgrade Supported Middleware, Software, Etc.

The Managed File Transfer Release Notes list the middleware and software supported by EquiSign. To upgrade non-EquiSign products, follow the instructions provided by the middleware or software vendor.